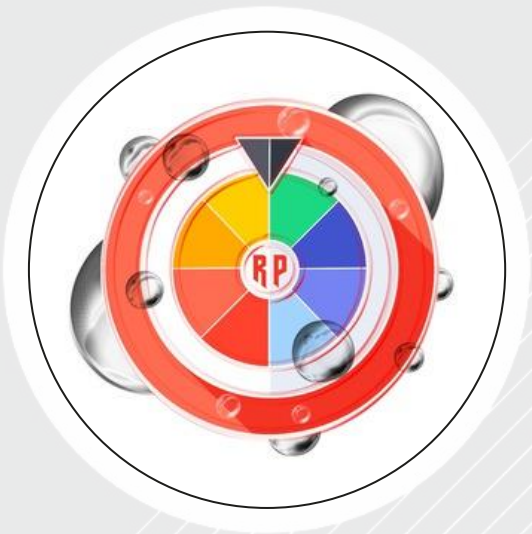
SPYWOLF

Security Audit Report



Completed on

August 4, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **Raffle Pot Grow** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

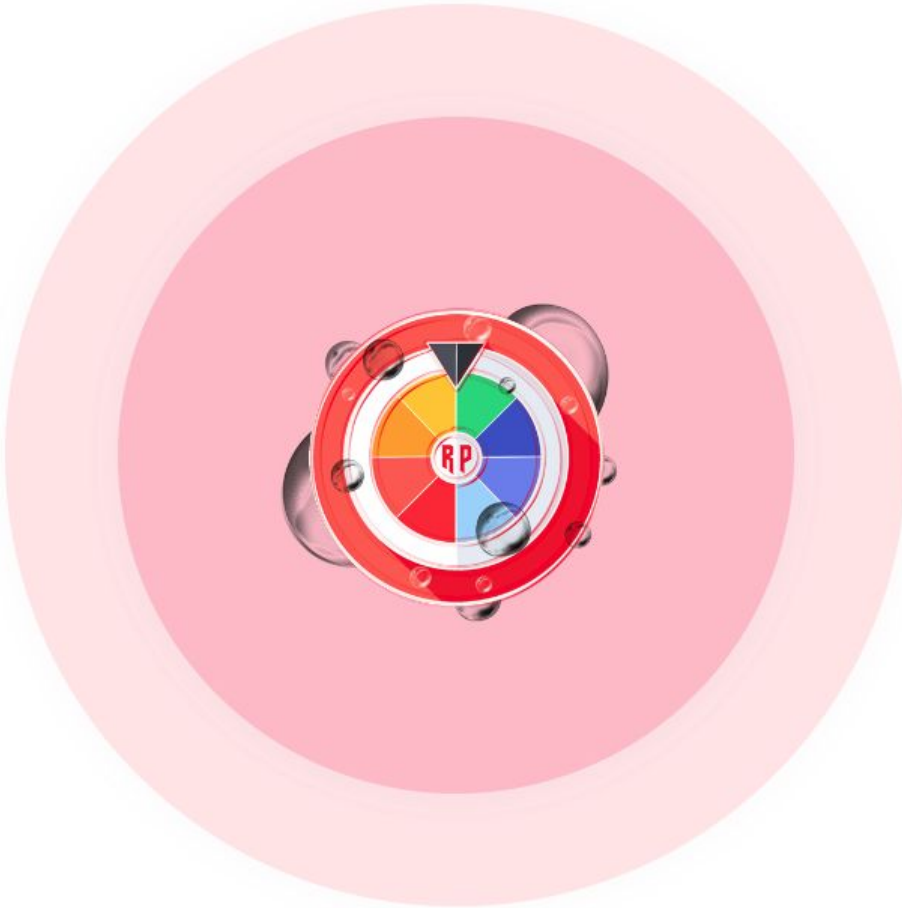
- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

RafflePotGrow



PROJECT DESCRIPTION

According to their whitepaper:

RafflePotGrow is a lottery token based on a daily automatic raffle. In order to join the daily raffles you need to hold a minimum amount of $RPG tokens in your wallet which will change based on the current daily market cap.

Release Date: Presale starts on August 04, 2022

Category: Lottery

CONTRACT INFO

Token Name
RafflePotGrow

Symbol
RPG

Contract Address
0x5b1c6f1a45EB55f2d680ef5Cd04F252cf85E5155

Network
Binance Smart Chain

Language
Solidity

Deployment Date
August 02, 2022

Verified?
Yes

Total Supply
1,000,000,000

Status
Not launched

TAXES

Buy Tax
12%

Sell Tax
14%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of August 04, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount

No Limit

DEX:

PancakeSwap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	2
Uniq Senders	2
Uniq Receivers	2
Total Amount	1999999999.9980001 RPG
Median Transfer Amount	1000000000 RPG
Average Transfer Amount	999999999.9990001 RPG
First transfer date	2022-08-02
Last transfer date	2022-08-02
Days token transferred	1

SMART CONTRACT STATS

Calls Count	8
External calls	4
Internal calls	4
Transactions count	5
Uniq Callers	2
Days contract called	1
Last transaction time	2022-08-02 23:11:19 UTC
Created	2022-08-02 22:02:13 UTC
Create TX	0x45cfe98d7d89ff8fdb78f7ae7ee0860d24562459bf800da02056e80d2bf132cc
Creator	0x436da93338e2f16fab9077d7a824f36585156829

FEATURED WALLETS

Owner address	0x436da93338e2f16fab9077d7a824f36585156829
Marketing wallet	0x5b516572aff1b984d01925e2ed37633e45c8d54f
Team wallet	0xbfc2ced48fd1365ac0acbd637045b1f67b3e330d
LP address	**Liquidity not added yet**

TOP 3 UNLOCKED WALLETS

1

100%

0xf63a1aCa0DF0fB95405EE7bd6A7C2bCCdaF94E65
Pinksale presale contract

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

⚠ Low Risk

Owner can exclude address from participating in lottery draws.

```
function excludeLotteryPartecipant(address account)public onlyOwner{
    lotteryParticipants.remove(account);
}
```

Owner can set token hold criteria to be eligible for lottery draws.

```
function setTokenAmountForLotteryParticipant(uint256 amount) external onlyOwner {
    tokenAmountForLotteryParticipant = amount * 10**_decimals;
}
```

Owner can change accumulated tokens criteria for lottery draw.

```
function setLotteryBalanceLimit(uint256 amount) public onlyOwner {
    lotteryBalanceLimit=amount;
}
```

Owner can withdraw accumulated lottery tokens from the contract.

```
function recoveryJackpot() public onlyOwner{
    lotteryBalance=0;
    uint256 amountJackpot = address(this).balance;
    address payable ownerWallet = payable(owner());
    transferToAddressETH(ownerWallet, amountJackpot);
}
```

⚠ Low Risk

Owner can buy taxes up to 12% and sell taxes up to 13%.
Combined buy+sell=25%.

```
function setBuyTaxes(uint256 newLiquidityTax, uint256 newMarketingTax,
uint256 newTeamTax,uint256 newJackPotTax) external onlyOwner() {
    require(newLiquidityTax.add(newMarketingTax).add(newTeamTax)
    .add(newJackPotTax) <= 12, "Tax exceeds the 12%.");
    _buyLiquidityFee = newLiquidityTax;
    _buyMarketingFee = newMarketingTax;
    _buyTeamFee = newTeamTax;
    _buyJackPotFee=newJackPotTax;

    _totalTaxIfBuying = _buyLiquidityFee.add(_buyMarketingFee)
    .add(_buyTeamFee).add(_buyJackPotFee);
}

function setSelTaxes(uint256 newLiquidityTax, uint256 newMarketingTax,
uint256 newTeamTax,uint256 newJackPotTax) external onlyOwner() {
    require(newLiquidityTax.add(newMarketingTax).add(newTeamTax)
    .add(newJackPotTax) <= 13, "Tax exceeds the 13%.");
    _sellLiquidityFee = newLiquidityTax;
    _sellMarketingFee = newMarketingTax;
    _sellTeamFee = newTeamTax;
    _sellJackPotFee=newJackPotTax;

    _totalTaxIfSelling = _sellLiquidityFee.add(_sellMarketingFee)
    .add(_sellTeamFee).add(_sellJackPotFee);
}
```

Informational

Owner can exclude address from fees.

```
function setIsExcludedFromFee(address account, bool newValue) public onlyOwner {
    isExcludedFromFee[account] = newValue;
}
```

Owner can initiate lottery draw.

```
function lotteryDraw() public onlyOwner{
    randNonce++;
    uint256 amountJackpot = address(this).balance;

    require(amountJackpot >= lotteryBalanceLimit, "Insufficient jackpot");

    if(amountJackpot > lotteryBalanceLimit)
        amountJackpot = amountJackpot.sub(amountJackpot.sub(lotteryBalanceLimit));

    uint256 partecipantWinner = uint256(keccak256(abi.encodePacked(block.timestamp,msg.sender,randNonce))) % lotteryParticipants.keys.length;
    bool winnerAvailable = false;

    for(uint256 i= 0;i<lotteryParticipants.keys.length;i++){
        if(lotteryParticipants.get(lotteryParticipants.keys[i])>=tokenAmountForLotteryParticipant){
            winnerAvailable=true;
        }
    }

    require(winnerAvailable,"No lottery participant present among the holders.");

    while(lotteryParticipants.get(lotteryParticipants.keys[partecipantWinner])<tokenAmountForLotteryParticipant)
        partecipantWinner = uint256(keccak256(abi.encodePacked(block.timestamp,msg.sender,randNonce))) % lotteryParticipants.keys.length;

    address payable winner= payable(lotteryParticipants.keys[partecipantWinner]);
    transferToAddressETH(winner, amountJackpot);
    lotteryBalance=lotteryBalance.sub(amountJackpot);
    emit winnerIs(winner,amountJackpot);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Raffle Pot Grow

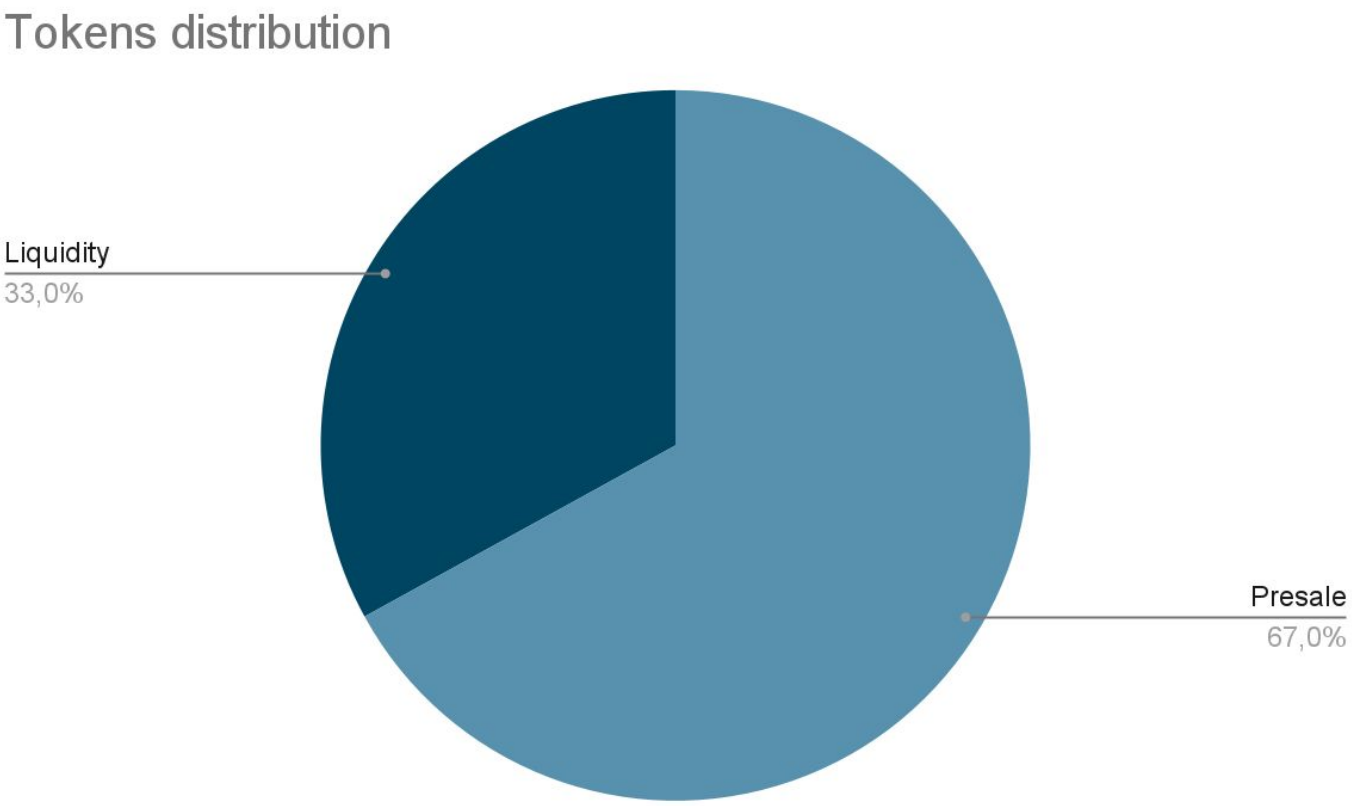
GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot stop or pause the contract
- ✔ The owner cannot set a transaction limit
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

*The following tokenomics are based on the pinksale's presale page:

- 67% - Presale
- 33% - Liquidity



THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.

WEBSITE

Website URL
https://rafflepotgrow.com

Domain Registry
http://www.register.it

Domain Expiration
Expires on 2023-08-01

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

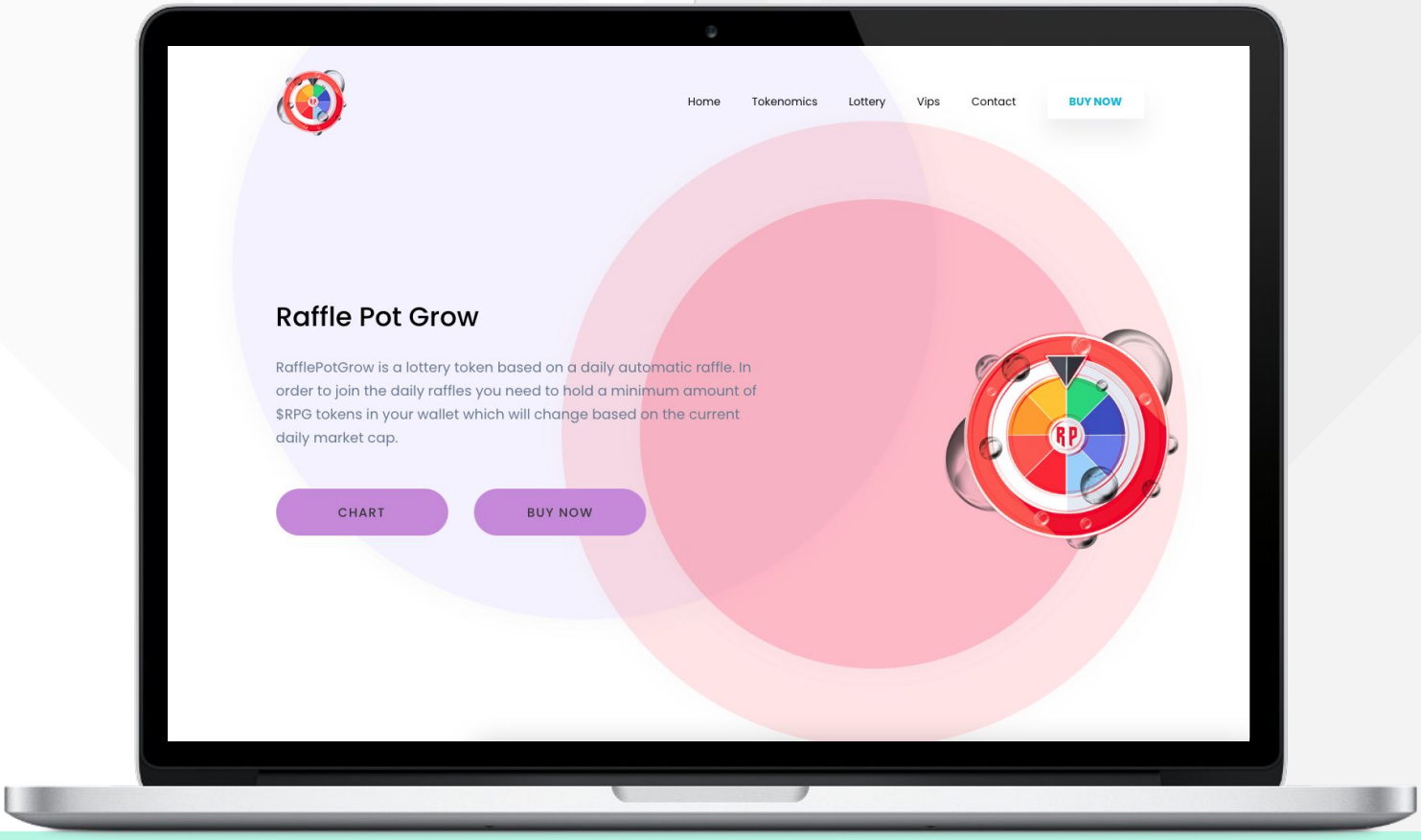
Design
Single page template design, appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written but a bit short.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes



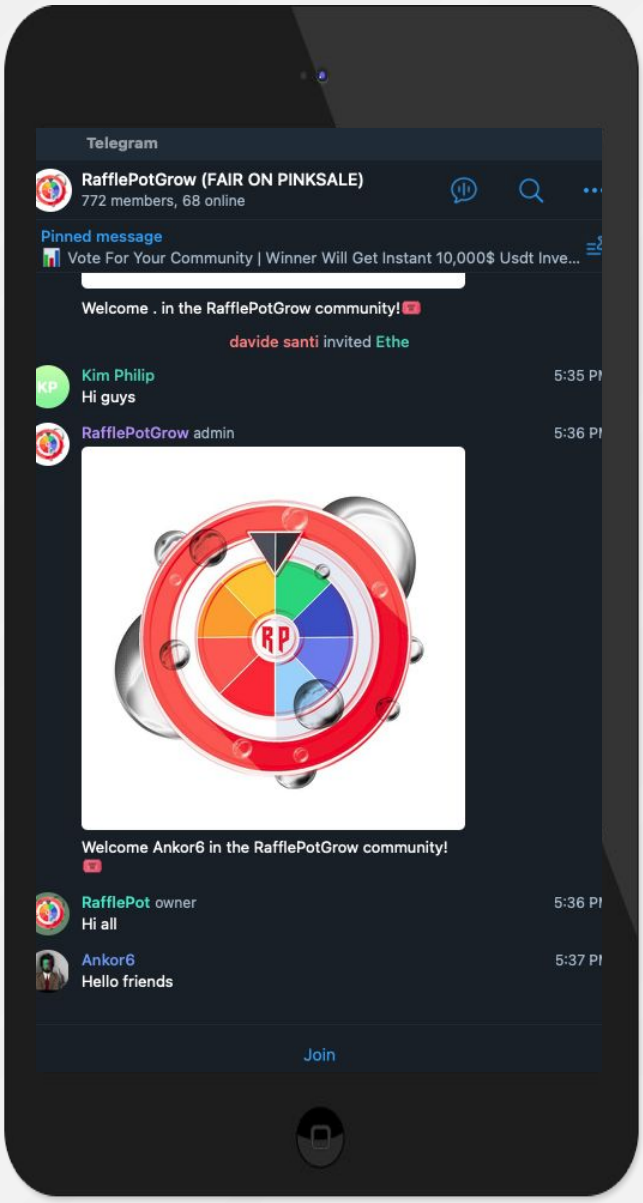
rafflepotgrow.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media activity is concentrated in telegram



Twitter

@RafflepotGROvv

- 8 followers
- 2 posts total
- New account

Discord

- Not available

Telegram

@RafflePotGrow

- 1 876 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.